APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/700,656	02/14/2001	Harald Vater	JEK/VATER	7577

7590   01/20/2011

Bacon & Thomas
Fourth Floor
625 Slaters Lane
Alexandria, VA 22314-1176

EXAMINER
DAVIS, ZACHARY A

ART UNIT	PAPER NUMBER
2492	

MAIL DATE	DELIVERY MODE
01/20/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	09/700,656	VATER ET AL.
	Examiner	Art Unit	
	Zachary A. Davis	2492	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>29 October 2010</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>26-33 and 42</u> is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>26-33 and 42</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1.   A request for continued examination under 37 CFR 1.114, including the fee set

forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this

application is eligible for continued examination under 37 CFR 1.114, and the fee set

forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action

has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 29

October 2010 has been entered.

2.   By the above submission, Claim 26 has been amended. No claims have been

added or canceled. Claims 26-33 and 42 are currently pending in the present

application.

Response to Arguments

3.   Applicant's arguments filed 29 October 2010 have been fully considered but they

are not persuasive.

       Regarding the rejection of Claims 26-33 and 42 under 35 U.S.C. 103(a) as

unpatentable over Kocher et al, US Patent Application Publication 2002/0124178, in

view of Cordery et al, US Patent 5655023, Applicant generally argues that although

Kocher discloses the steps of falsifying and combining as claimed, and Cordery does

disclose pre-computation of secret data, the references cannot be combined to result in the claimed invention (see pages 4-12 of the present response).

In particular, Applicant states that the issue in the present case is "whether Cordery would have led one of ordinary skill in the art to modify Kocher's method by replacing contemporaneous auxiliary function value generation with predetermined auxiliary function values and retrieval of the auxiliary values before beginning data falsification" (see page 10 of the present response, emphasis removed). The Examiner agrees that this is the primary issue to be resolved. Although Applicant states that this issue must be answered in the negative, the Examiner respectfully disagrees, and submits that the teachings of Cordery in combination with the method of Kocher would indeed have led one of ordinary skill to use pre-calculated auxiliary values rather than calculating them on the fly, in order to protect the algorithm and secret key used (see Cordery, column 3, lines 11-13, as previously cited).

More specifically, first, Applicant argues that the Examiner's alleged analysis that "Cordery's teaching of a postal meter that includes a removable token for storing secret keys would have cause [sic] the ordinary artisan to modify Kocher's method differential power analysis method [sic] by eliminating the auxiliary function value generation step and instead use a pre-stored auxiliary function value.... makes no sense" (see page 5 of the present response). It is noted that the previous Office action did not provide the specific analysis/conclusion that Applicant alleges, but rather relied upon the broader teaching in Cordery of secret function values being pre-computed (as previously cited, see Cordery, column 3, lines 18-25, where tokens are pre-computed, see also column

5, lines 10-12, where tokens include encrypted data, and column 3, lines 11-13, where

the encryption algorithm and keys are protected). Applicant further asks "[b]y what logic

would one of ordinary skill in the art decide that Cordery's general key storage

arrangement… suggests modification of the power-analysis-preventing algorithm, when

Kocher already includes a key storage arrangement… and does not use it to modify the

… algorithm" (pages 5-6 of the present response, emphasis removed). The Examiner

fails to appreciate this argument, as it is not clear what Applicant is referring to by "using

a key storage to modify a power-analysis-preventing algorithm" or how Applicant is

proposing such a modification would be made. Further, although Applicant refers to

"key storage arrangement 290" in Kocher, element 290 is more broadly and simply

described as "memory" and which is explicitly described as storing "the key **and/or**

other information" (see Kocher, paragraph 0051, emphasis added). Clearly, this

memory is generally used by the processor throughout the encryption processes which

are the subject of the power analysis prevention, which makes it difficult to apprehend

why Applicant suggests that the memory is not used in Kocher's algorithm.

        Applicant further argues that Cordery "has nothing to do with power analysis"

(page 6 of the present response). Although Applicant states that it is not being argued

that Cordery is non-analogous art (page 5 of the present response), the statement that

Cordery has nothing to do with power analysis (such as that described in Kocher or the

present application) appears to amount to such an argument. Therefore, the Examiner

repeats that, in response to applicant's argument that Cordery is nonanalogous art, it

has been held that a prior art reference must either be in the field of applicant's

endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, Cordery is concerned with the encryption and protection of secret data (see, for example, column 3, lines 18-58). This is reasonably pertinent to the problem with which Applicant is concerned, namely the prevention of leakage of secret information (see page 1 of the present specification), and therefore one of ordinary skill in the art would have reasonably looked to Cordery when considering the problem with which Applicant is concerned. See also MPEP § 2141.01(a). "Under the correct analysis, any need or problem known in the field of endeavor at the time of the invention and addressed by the patent [or application at issue] can provide a reason for combining the elements in the manner claimed." *KSR International Co. v. Teleflex Inc.*, 550 U.S. ___, ___, 82 USPQ2d 1385, 1397 (2007). Thus a reference in a field different from that of applicant's endeavor may be reasonably pertinent if it is one which, because of the matter with which it deals, logically would have commended itself to an inventor's attention in considering his or her invention as a whole. (It is noted that, in footnote 1, page 5 of the present response, Applicant appears to misconstrue the Examiner's previous statement regarding non-analogous art as stating that any techniques of data protection are combinable; however, the Examiner was not alleging such a broad conclusion. Rather, the Examiner was more narrowly stating that, because Cordery is directed to encryption and protecting and keeping secret data required for performing such encryption, this would be reasonably pertinent to

Applicant's concern of preventing the leakage of secret information, and one of ordinary

skill would have reasonably considered the reference in considering the problem at

hand).

　　　Applicant further appears to allege that one of the references teaches away from

their combination, since Cordery teaches key storage and "an aspect" of Kocher's

method "has nothing to do with key storage" (see page 6 of the present response, citing

MPEP § 2141.02). However, Applicant does not appear to have clearly cited any

particular evidence from Cordery or Kocher that would teach away from the

combination. Further, even if such evidence were present, there does not appear to be

any disclosure in Kocher or Cordery that constitutes a teaching away from their

combination because a teaching away requires the disclosure to "criticize, discredit, or

otherwise discourage the solution claimed." *In re Fulton*, 391, F.3d 1195, 1201, 73

USPQ2d 1141, 1146 (Fed. Cir. 2004). See also MPEP § 2145(X)(D). It is further noted

that the references to "the Turk patent" and "reel sensing devices" (page 6 of the

present response) do not appear to have any relevance to the present application.

　　　Applicant additionally argues that the blinding is only performed after performing

an additional permutation and that this is essential to the method of Kocher and cannot

be omitted without rendering Kocher's method inoperative (pages 6-7 of the present

response). However, there is nothing in Kocher to prevent the blinding data or the

permutation data or both from being previously computed. Applicant appears to argue

that the permutation could not be computed beforehand, but there is nothing that

explicitly prevents this. Again, Cordery is seen as providing a general teaching that

security related computations could be done prior to when they are needed in secure surroundings (Cordery, column 3, lines 18-25; column 5, lines 10-12; and column 3, lines 11-13; see also column 4, lines 52-59, as previously cited); therefore, this would be suggestive of pre-computing any of the needed function values, including, without limitation, the random blinding bit b and the random permutation *perm*, as well as the unblinding vector. Applicant states that "Cordery merely teaches that keys **and other secret data** can be stored" (page 7 of the present response, emphasis altered); however, the Examiner submits that not only does Cordery teach storing the keys and other secret data (which one of ordinary skill in the art, considering the method of Kocher, would recognize to include the blinding and/or permutation data), but Cordery also discloses the pre-calculation of such data (again, Cordery, column 3, lines 18-25; column 5, lines 10-12; and column 3, lines 11-13; see also column 4, lines 52-59, as previously cited).

Applicant further argues that the blinding/falsifying operations in Kocher must be performed after the permutation and that interchanging their order would be contrary to the teachings of Kocher (pages 7-8 of the present response). However, although the claim states that the falsifying is performed before execution of one or more operations, this does not preclude the performance of other operations prior to the falsifying step. Further, Kocher discloses both permuting (with randomized ordering) and blinding the data (Kocher, paragraph 0070-0072, for example) and that data can be maintained in the blinded state during processing, for example, for multiple permutations, until

nonlinear operations need to be performed (Kocher, paragraph 0074); that is, permutations can also be performed after the blinding.

Applicant further details a list of changes that would allegedly need to be made to modify Kocher in order to obtain the claimed invention (pages 8-9 of the present response); however, again, the Examiner notes that these changes all appear to be largely conjecture. Additionally, even assuming *arguendo* that the changes are required, these changes are further suggested by Cordery. Specifically, the general teachings of Cordery would have suggested to one of ordinary skill that any number of security-related function values, such as the blinding bits and unblinding bits and any other data needed for these calculations such as the permutation could be pre-computed in secure surroundings and stored securely (Cordery, column 3, lines 18-25; column 5, lines 10-12; and column 3, lines 11-13; see also column 4, lines 52-59, as previously cited), in order to protect the encryption algorithm and secret key used (see Cordery, column 3, lines 11-13).

Applicant again argues that in the claimed invention would not have resulted from the changes to Kocher as suggested by Applicant (pages 8-9 of the present response, as noted above) because the blinding step occurs only after permutation and because the permutation serves a specific security purpose (pages 9-10 of the present response; no evidence is cited for what such a security purpose would be). However, it is again noted that Kocher discloses both permuting (with randomized ordering) and blinding the data (Kocher, paragraph 0070-0072, for example) and that data can be maintained in the blinded state during processing, for example, for multiple permutations, until

nonlinear operations need to be performed (Kocher, paragraph 0074). That is, Kocher

discloses that the blinding can occur before additional permutations (corresponding to

the claimed executed operations) take place (Kocher, paragraph 0074).

Applicant further argues that "Cordery does not teach that there is a risk to

generating auxiliary function values" (page 10 of the present response); however, the

Examiner fails to appreciate the relevance of this argument. Applicant additionally

argues that Kocher is not concerned with the protection of pre-stored data (page 10 of

the present response); however, it is noted that Cordery discloses exactly this (again,

Cordery, column 3, lines 18-25; column 5, lines 10-12; and column 3, lines 11-13; see

also column 4, lines 52-59, as previously cited).

Applicant again acknowledges that Kocher and the present application "are

concerned with the discovery of data protection algorithms, and the secret key used

therein, by analyzing power emissions" and that Kocher teaches one method that

generates auxiliary values during data falsification and the claimed invention

predetermines the auxiliary values (page 10 of the present response). Applicant further

questions what advantage the modification of Kocher to include pre-calculation of

auxiliary values would be recognized, asserting that protection against discovery of

secret data was "clearly not a problem in the secure system of Cordery" (page 11 of the

present response). However, Cordery does indeed recognize the need to protect

encryption algorithms and secret keys used therewith (Cordery, column 3, lines 11-13).

Applicant once again argues that Cordery does not use auxiliary function values

(page 11 of the present response). In response to applicant's arguments against the

references individually, one cannot show nonobviousness by attacking references

individually where the rejections are based on combinations of references. See *In re*

Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091,

231 USPQ 375 (Fed. Cir. 1986). The Examiner notes that Kocher does disclose the

use of auxiliary function values as claimed (Kocher, paragraphs 0070, 0072, and 0073,

as previously cited).

Applicant again argues that Cordery teaches storage of sensitive pre-determined

data but does not teach replacing a particular item of sensitive data required by Kocher

should be replaced by pre-stored data (page 11 of the present response). However,

once again, the Examiner notes that the general teachings of Cordery would have

suggested to one of ordinary skill that any number of security-related function values,

such as the blinding bits and unblinding bits and any other data needed for these

calculations such as the permutation could be pre-computed in secure surroundings

and stored securely (Cordery, column 3, lines 18-25; column 5, lines 10-12; and column

3, lines 11-13; see also column 4, lines 52-59, as previously cited), in order to protect

the encryption algorithm and secret key used (see Cordery, column 3, lines 11-13). As

per MPEP § 2141.03(I), "A person of ordinary skill in the art is also a person of ordinary

creativity, not an automaton." *KSR International Co. v. Teleflex Inc.*, 550 U.S. ___, ___,

82 USPQ2d 1385, 1397 (2007). "[I]n many cases a person of ordinary skill will be able

to fit the teachings of multiple patents together like pieces of a puzzle." *Id.* Office

personnel may also take into account "the inferences and creative steps that a person

of ordinary skill in the art would employ." *Id.* at ___, 82 USPQ2d at 1396. Therefore, the

Examiner submits that one of ordinary skill would have recognized that Cordery is

suggestive of pre-computation of any security-related function value, including those

taught by Kocher, and thus the combination of Kocher as modified by Cordery would

have suggested the claimed invention.

Applicant further argues that the secret data to be protected in Cordery is not

stored on the data carrier but rather on a separate secure co-processor (see pages 11-

12 of the present response, citing Cordery, column 9, line 66-column 10, line 61, and

Figure 5). However, Cordery does disclose that secret data is pre-computed and stored

on data carriers (see, for example, column 4, lines 52-59, where pre-computed tokens

are stored on smart cards, corresponding to the claimed data carrier). Further, the use

of the secure co-processor in Cordery corresponds to the previous computation in safe

surroundings as claimed (see Cordery, column 9, line 66-column 10, line 61, as cited,

where the secure co-processor generates the tokens, and then the pre-computed

tokens are transferred for storage to the storage device 104, corresponding to the

claimed data carrier). It is noted that "safe surroundings" are not explicitly defined or

discussed in detail in the present specification, and therefore, the term has been broadly

construed. It is certainly reasonable to conclude that a secure co-processor within

tamper-proof surroundings would be considered "safe surroundings" for performing

security-related calculations.

Additionally, Applicant again argues that the method of Kocher is "fundamentally

different" than the claimed method (page 12 of the present response); however,

Applicant has also acknowledged that Kocher discloses the two positively recited steps

of the claimed method, namely the falsifying and combining/compensation (for example, see page 5 of the previous response). Therefore, the Examiner disagrees that the methods are fundamentally different. Further, Applicant again argues that Cordery only teaches pre-computation in the context of a secure co-processor (page 12 of the present response); however, again, it is noted that this appears to correspond to the claimed limitation that the previous computation of the values is performed in "safe surroundings". Further, as noted above, Cordery is seen to teach, in general, the pre-computation of security-related function values, and in combination with the disclosed steps of Kocher, it is submitted that this would have suggested the claimed invention to one of ordinary skill in the art at the time the invention was made.

Finally, it is generally noted that Applicant provides numerous statements as to whether a combination of references would be inoperable and also submits various other characterizations of the references without providing any evidence in support thereof. The arguments of counsel cannot take the place of evidence in the record. *In re Schulze*, 346 F.2d 600, 602, 145 USPQ 716, 718 (CCPA 1965). See MPEP § 716.01(c)(II). More specifically, arguments of counsel cannot take the place of factually supported objective evidence. See, e.g., *In re Huang*, 100 F.3d 135, 139-40, 40 USPQ2d 1685, 1689 (Fed. Cir. 1996); *In re De Blauwe*, 736 F.2d 699, 705, 222 USPQ 191, 196 (Fed. Cir. 1984). See MPEP § 2145. An argument does not replace evidence where evidence is necessary; attorney argument is not evidence unless it is an admission. The arguments of counsel cannot take the place of evidence in the record. *In re Schulze*, 346 F.2d 600, 602, 145 USPQ 716, 718 (CCPA 1965); *In re Geisler*, 116

F.3d 1465, 43 USPQ2d 1362 (Fed. Cir. 1997) ("An assertion of what seems to follow

from common experience is just attorney argument and not the kind of factual evidence

that is required to rebut a prima facie case of obviousness."). See MPEP § 2145(I).

Therefore, for the reasons detailed above, the Examiner maintains the rejection

as set forth below.

Claim Rejections - 35 USC § 101

4.   The rejection of Claims 26-33 and 42 under 35 U.S.C. 101 as directed to non-

statutory subject matter is withdrawn in light of the amendments to the claims. The

Examiner notes that the step of retrieval of a function value from a memory is only

directed to insignificant extra-solution activity (see page 6 of the Interim Instructions,

where gathering of data is explicitly described as insignificant extra-solution activity);

however, the additional step of the execution of operations on a semiconductor chip

clearly limits the method, and thus clearly ties the performance of the method to a

particular machine.

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set
forth in section 102 of this title, if the differences between the subject matter sought to be patented and
the prior art are such that the subject matter as a whole would have been obvious at the time the

> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

6.   Claims 26-33 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Kocher et al, US Patent Application Publication 2002/0124178, in view of Cordery

et al, US Patent 5655023.

In reference to Claim 26, Kocher discloses a method of protecting secret data

stored in a semiconductor chip of a data carrier, where the method includes falsifying

input data by combination with auxiliary data before execution of one or more

operations and executing those operations on the semiconductor chip (paragraphs

0068, 0070, and 0072, where blinding occurs before permutation operations), and

combining the output data with an auxiliary function value in order to compensate for the

falsification of the input data (paragraphs 0070, 0072, and 0073, where unblinding

occurs to compensate for the blinding), where the auxiliary value was determined by

executing the operations using the auxiliary data as input data (paragraph 0072, where

the output buffer is initialized with the blinding bit and the data in the output buffer is the

result of using the input permutation table, i.e. the operations). However, while Kocher

discloses previously determining the auxiliary data and/or values (see paragraph 0072),

Kocher does not explicitly disclose determining the auxiliary value previously and in safe

surroundings.

Cordery discloses a method in which secret function values are pre-computed in

safe surroundings and where the secret values are maintained securely, i.e. stored in

the memory of a semiconductor chip of a data carrier, and then later retrieved for use

(see column 3, lines 18-25, where tokens are pre-computed, see also column 5, lines

10-12, where tokens include encrypted data, and column 3, lines 11-13, where the

encryption algorithm and keys are protected; see also column 4, lines 52-59, where the

tokens are stored on smart cards and protected against tampering, i.e. maintained

securely). Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to modify the method of Kocher to include pre-computation

and safe storage of secret function values in order to protect the encryption algorithm

and secret key used (see Cordery, column 3, lines 11-13).

        In reference to Claim 27, Kocher and Cordery further disclose that the

combination with the auxiliary function value is performed before execution of a non-

linear operation (see Kocher, paragraph 0074, where inputs can be maintained in a

blinded state and only reconstituted when nonlinear operations must be performed).

        In reference to Claim 28, Kocher and Cordery further disclose that the auxiliary

data are varied and function values are stored in the memory of the data carrier

(Kocher, paragraphs 0072-0075; Cordery, column 4, lines 54-58).

        In reference to Claims 29-32, Kocher and Cordery further disclose that new

auxiliary values can be generated by combining existing values, that auxiliary data are

selected randomly, pairs of auxiliary data and auxiliary function values are generated,

and the auxiliary data are random numbers (see Kocher, paragraphs 0072 and 0075).

        In reference to Claim 33, Kocher and Cordery further disclose combining the

output data and auxiliary function value using an XOR operation (see Kocher,

paragraph 0073).

In reference to Claim 42, Kocher and Cordery further disclose that operations include permutations of data (see Kocher, paragraphs 0068 and 0070-0074).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 9:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Thomas can be reached on (571) 272-6776. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Zachary A Davis/
Primary Examiner, Art Unit 2492